(19) 日本国特許庁 (JP)

(12) 公開特許公報（A）

(11) 特許出願公開番号

特開２００１－２３６３２５
（Ｐ２００１－２３６３２５Ａ）
(43) 公開日 平成13年8月31日(2001.8.31)

(51)Int.Cl.[7]		識別記号	FI			テーマコード(参考)
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０ Ｇ	5B085
	1/00	３７０		1/00	３７０ Ｅ	5J104
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７３ Ａ	
					６７３ Ｅ	
					６７３ Ｃ	

審査請求 未請求 請求項の数 １４ ＯＬ （全 １２ 頁）

(21) 出願番号 特願2000-45634(P2000-45634)

(22) 出願日 平成12年2月23日(2000.2.23)

(71) 出願人 599094901
株式会社メリッツ
埼玉県川越市的場1361－1

(72) 発明者 是安 俊之
埼玉県川越市的場1361－1 株式会社メリッツ内

(74) 代理人 100103160
弁理士 志村 光春

Ｆターム(参考) 5B085 AE02 AE11 AE23
5J104 AA07 KA01 KA21 NA05 NA12

(54)【発明の名称】個人識別システムおよびその使用方法

(57)【要約】
【課題】電子システムを操作しようとしている者を、間違いなく本人識別され得る機能を、低コストで、確実に、しかも操作者にとって簡便に実行され得る手段を提供すること。
【解決手段】①個人識別情報を発信する赤外線通信機構ａを有する小型端末１、および、②赤外線通信機構ａを介した個人識別情報の情報交換をすることが可能な赤外線通信機構ｂを有する個人識別端末２を要素として含み、この個人識別端末２において、前記の個人情報の内容に応じて個人の識別を行う個人識別システム、並びに、この個人識別システムの多様な使用方法を提供することにより、上記の課題を解決し得ることを見出した。

【特許請求の範囲】

【請求項１】①個人識別情報を発信する赤外線通信機構ａを有する小型端末１、および、②赤外線通信機構ａを介した個人識別情報の情報交換をすることが可能な赤外線通信機構ｂを有する個人識別端末２を要素として含み、この個人識別端末２において、前記の個人情報の内容に応じて個人の識別を行う個人識別システム。

【請求項２】個人識別情報を赤外線通信機構ａから発信させ、この個人識別情報を赤外線通信機構ｂが受信し、かつ、かかる個人識別情報が個人識別端末２における照合により適合とされた場合にのみ、個人識別端末２が本人識別肯定時の反応をすることにより個人の識別を行う、請求項１記載の個人識別システムの使用方法。

【請求項３】赤外線通信機構ａにおける個人識別情報の発信が間欠的な発信であり、かつ、①個人識別端末２における照合により、この間欠的に発信された個人識別情報が不適合とされた時点で、および／または、②個人識別端末２が、この間欠的に発信された個人識別情報を受信できなくなった時点で、個人識別端末２が本人識別否定時の反応をすることにより個人の識別を行う、請求項２記載の個人識別システムの使用方法。

【請求項４】個人識別情報にランダムデータが含まれ、このランダムデータの照合を個人の識別行為に含めて個人を識別する、請求項２または３記載の個人識別システムの使用方法。

【請求項５】ランダムデータが、ワンタイムパスワード、一方向ハッシュ関数の出力値および擬似乱数発生プログラムにより得られる擬似乱数からなる群から選ばれる１種または２種以上のランダムデータである、請求項４記載の個人識別システムの使用方法。

【請求項６】個人識別情報に暗号化されている情報が含まれ、この暗号化されている情報を照合して個人を識別する、請求項２～５のいずれかの請求項記載の個人識別システムの使用方法。

【請求項７】応答要求メッセージを赤外線通信機構ｂから発信させ、この応答要求メッセージを赤外線通信機構ａが受信した場合に、小型端末１から個人識別端末２に向けて応答メッセージを送信させ、この応答メッセージが個人識別端末２において適合とされた場合にのみ、個人識別端末２が本人識別肯定時の反応をすることにより個人の識別を行う、請求項１記載の個人識別システムの使用方法。

【請求項８】個人識別端末２が個人を識別している場合のみ、この個人識別端末２に、識別対象の小型端末１に対して特異的な応答要求メッセージを発信させて、これにより小型端末１を、かかる個人識別端末２からの特異的な応答要求メッセージのみに対して応答メッセージを発信するようにし、さらに個人識別端末２を、この小型端末１からの応答メッセージのみに呼応可能な状態とし、かつ、個人識別端末２が個人を識別していない場合

には、個人識別端末２に、不特定の小型端末１に対する応答要求メッセージを発信させ、小型端末１を、この対象不特定の応答要求メッセージのみに呼応可能な状態とする、請求項７記載の個人識別システムの使用方法。

【請求項９】応答要求メッセージおよび／または応答メッセージに、ランダムデータが含まれ、このランダムデータの照合を個人の識別行為に含めて個人を識別する、請求項７または８記載の個人識別システムの使用方法。

【請求項１０】ランダムデータが、ワンタイムパスワード、一方向ハッシュ関数の出力値および擬似乱数発生プログラムにより得られる擬似乱数からなる群から選ばれる１種または２種以上のランダムデータである、請求項９記載の個人識別システムの使用方法。

【請求項１１】応答要求メッセージおよび／または応答メッセージに暗号化されている情報が含まれ、この暗号化されている情報を照合して個人を識別する、請求項９または１０のいずれかの請求項記載の個人識別システムの使用方法。

【請求項１２】応答要求メッセージの発信が間欠的な発信であり、かつ、①これに対する応答メッセージが個人識別端末２において不適合とされた時点で、および／または、②これに対する応答メッセージを、個人識別端末２が受信できなくなった時点で、個人識別端末２が本人識別否定時の反応をすることにより個人の識別を行う、請求項７～１１のいずれかの請求項記載の個人識別システムの使用方法。

【請求項１３】個人識別端末２から間欠的に発信される応答要求メッセージの一部に応答要求メッセージ毎に異なる情報が含まれており、かつ、個々の応答要求メッセージに対して小型端末１から発信される応答メッセージに、前記の情報を若しくはこの情報を加工した情報を暗号化した情報が含まれており、この応答メッセージを個人識別端末２が受信した際に、前記の暗号化された情報を複号して、この複号情報と前記の応答要求メッセージに含まれる情報と比較照合して、両情報が実質的に同一である場合に、個人識別端末２が本人識別肯定時の反応を行う、請求項７～１１のいずれかの請求項記載の個人識別システムの使用方法。

【請求項１４】小型端末１と個人識別端末２が、同一のランダムデータの発生プログラムを保有し、個人識別端末２と小型端末１との間の初期の応答要求メッセージおよび／または応答メッセージに含まれる暗号化されている情報に、前記のランダムデータのシード値となる値を含ませ、以後、小型端末１から個人識別端末２に向けて送られるメッセージに、このシード値を初期値として発生させたランダムデータを含ませ、個人識別端末２においても前記のランダムデータの発生プログラムにより前記のシード値を初期値としたランダムデータを算出し、小型端末１から個人識別端末２に向けて送られる前記のメッセージに含まれるランダムデータと比較照合して、

両者のランダムデータが一致した場合に、個人識別端末２が本人識別肯定時の反応をする、請求項７～１２のいずれかの請求項記載の個人識別システムの使用方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子端末において個人を識別するためのシステムと、その使用方法に関する発明である。さらに具体的には、本発明は、赤外線通信機能を用いた前記システムと、その使用方法に関する発明である。

【０００２】

【従来の技術】従来、電子端末における個人の識別手段として最も広く利用されてきたのは、パスワードによる個人識別である。この手法は、一般に、コンピュータのキーボードからその個人のＩＤ情報（例えば、社員番号）とパスワード（暗証番号等）を入力し、それらが事前にコンピュータに登録されているものと一致していれば操作している者が本人であると認め、その後の操作を許可するというものである。

【０００３】次に、磁気カードやＩＣカードに、ＩＤ情報やパスワード等を登録しておき、これをコンピュータに接続されたカード読み取り装置で読み取らせて、個人を識別する方法や、これと上記のキーボード入力を組み合わせた方法等が挙げられる。これらにより、例えば、パスワード等が他人に漏洩しても、カードを持った人間でなければ操作できないよう、安全性を高め、また、ＩＤ情報等をキーボードから入力する手間を軽減することも可能となった。

【０００４】また、最近は、指紋を読み取ったり、目の虹彩のパターン、声紋等といった、いわゆる生体情報により個人識別をする技術が開発されつつある。カードだと盗まれたり、偽造されたりする危険性もあるが、生体情報であれば、この点において安心である。

【０００５】しかし、これらの方法には、いずれも後述するような問題点が認められる。

【０００６】

【発明が解決するための課題】従来の個人識別方法には、一つ、決定的な問題点が認められる。それは、識別時に、識別対象者がそれを意識し、なんらかの操作をすることが必要であることである。つまり、電子端末の操作を開始する前に、パスワードをキーボードから入力し、離席時には、その後、他人に使用されないように終了処理をして、パスワードを再度入力しないと操作が再開できない状態にしなければならない。カードを用いる場合も同様であり、操作開始前にカードを読み取り装置に挿入し、離席時にはカードを抜き取って携帯しなければならない。生体情報の場合も、操作前に、例えば、指紋読み取り装置に指を数秒押し当てる等の操作をしなければならない。

【０００７】これらの個人識別方法は、一旦、個人識別

が完了すると、同様の状態が長時間継続し、識別対象者がめったに離席しないような場合であれば、何とか使用に耐え得るが、識別対象者の業務の性格によっては、頻繁に離席することも想定される。このような離席が頻繁である場合等は、着席する毎に同様の個人識別操作を行わなければならない。このような場合、人間は煩わしい作業を基本的に嫌うので、ついつい終了処理を怠ったりカードを挿入したままで席を離れたりして、離席中に他人にデータを盗み見られたり改竄されたりといった事故の可能性が非常に高くなってしまう。いくら高価で高度な識別システムを導入しても、カードが挿入されたままといった運用がなされると、個人識別のセキュリティー機能が全く無意味になってしまうこととなる。

【０００８】従って、この個人識別という作業は、操作者に特別な操作をさせることなく、できれば、識別対象者が全く意識しないうちに、システムが自動的に行ってくれるのが理想的であり、これが実現されることにより運用面も含めた個人識別システム全体の安全性を確保することが可能となる。

【０００９】非接触型のＩＣカードをこのような用途に使えないか検討したが、このようなＩＣカードは、カードに埋め込まれた小型のコイルを介して電磁波によって通信する仕組みであり、送受信装置が高価かつ大型になってしまう。よって、非接触型のＩＣカードは、駅の改札や高速道路の料金所等での利用には適しているが、例えば、オフィス内の全てのコンピュータ端末に設置するには無理がある。また、電磁波は指向性のコントロールや遮蔽が難しく、個々の通信エリアを明確に区分することが困難である。そのため、オフィス内のようにコンピュータ端末が密に配置され、また、ノート型ＰＣの普及により頻繁に移動もするというような運用環境において、コンピュータ端末群が相互に干渉されずに通信することは極めて困難である。

【００１０】

【課題を解決するための手段】本発明者は、鋭意検討の結果、赤外線通信を個人識別システムに用いることにより、上記の課題を解決可能であることに想到した。

【００１１】赤外線通信は、テレビやビデオのリモコンで広く普及しており、室内等における近距離通信には、最も広く使われている技術の一つである。最近のノート型パソコンには、ほとんど標準で赤外線通信装置が装備されており、ポケットに入るような携帯情報端末や携帯ゲーム機といった小型のコンピュータにも、赤外線通信装置が装備されているものが広く普及してきた。また、これらの携帯型のコンピュータと一般のコンピュータやネットワークとが、赤外線通信によって情報交換するための装置やソフトも普及し、情報交換の標準規約も、IrDA等いくつか制定されている。従って、赤外線通信によって自動的な個人識別を可能とすることは、既存の汎用技術に適切なソフトウェアを用いるだけで、上述した個

人識別に関する課題を解決することを意味する。

【００１２】また、赤外線は一種の光であるので、赤外線通信装置の通信可能範囲をコントロールするのが容易である。すなわち、赤外線通信装置の通信可能範囲は、基本的には、赤外線通信装置の受発光装置部分が互いに見える範囲（数センチから数メートル程度）であり、紙一枚でも簡単に遮蔽することが可能である。また、レンズや鏡等の一般の光学的道具を利用することによっても、簡単かつ安価に自由度の高い通信可能範囲設定を行うことができる。

【００１３】具体的には、本発明者は、本願において、①個人識別情報を発信する赤外線通信機構ａを有する小型端末１、および、②赤外線通信機構ａを介した個人識別情報の情報交換をすることが可能な赤外線通信機構ｂを有する個人識別端末２を要素として含み、この個人識別端末２において、前記の個人情報の内容に応じて個人の識別を行う個人識別システム（以下、本識別システムともいう）、並びに、このシステムの種々の使用方法（以下、本システム使用方法ともいう：さらに具体的には、後述する）を提供する。

【００１４】

【発明の実施の形態】以下、図面を用いつつ、本発明の内容について説明する。第１図は、本認識システムの概要を示す図面（正面図）である。

【００１５】第１図に表示する本認識システム１００は、①上記の赤外線通信機構ｂである赤外線受発光装置１１が接続され、少なくとも、この赤外線受発光装置１１からの電子情報を処理して個人を識別するソフトウエアが組み込まれた、上記の個人識別端末２として働くコンピュータ１０、並びに②上記の赤外線通信機構ａである赤外線受発光装置２１が組み込まれた上記の小型端末１として働く小型コンピュータ２０（第１図において、小型コンピュータ２０は、識別対象者３０によって携帯されている）によって構成されている。

【００１６】本認識システム１００を用いる場合には、少なくとも、赤外線受発光装置１１が赤外線による通信が可能な状態となっており、識別対象者３０は、小型コンピュータ２０を携帯し、これに設けられている赤外線受発光装置２１もまた、原則として赤外線による通信が可能な状態となっている。

【００１７】ここで、上記の個人識別端末２の種類としては、個人を認識して作動させる電子端末であれば、特に限定されるものではなく、第１図に示したようなコンピュータをはじめとして、ネットワーク端末、セキュリティー付加装置などを例示することができる。

【００１８】ここで、セキュリティー付加装置とは、他の装置に本発明の機能を付加する装置のことである。例えば、伝統的なタイプのコンピュータでは、これに赤外線通信機構ｂを接続できない場合や、個人の識別に必要なソフトウエアを実装できない場合も考えられる。このような場合に、個人の識別に必要な最低限の機能を実装した小型のコンピュータに、このコンピュータが制御可能なスイッチボックスを接続したものを、セキュリティー付加装置として用いることができる。ここに例示したセキュリティー付加装置では、キーボードやディスプレイをスイッチボックスを経由して、前記のような伝統的なタイプのコンピュータ本体と接続することで、本認識システムによる優れた安全性をこのコンピュータに付与することができる。すなわち、個人識別肯定時には、セキュリティー付加装置は、そのスイッチボックスのスイッチをＯＮの状態にして、キーボードによる操作やディスプレイの表示が可能なようにし、かつ、個人識別否定時には、前記スイッチをＯＦＦの状態にして、キーボードによる操作やディスプレイの表示を不能にすることができる。この場合、前記の伝統的なタイプのコンピュータで動いている業務プログラムの終了等の制御をすることはできないが、操作や表示を制御するだけでも十分なセキュリティーの確保ができる場合が多いので、十分に有用である。このようなセキュリティー付加装置を、例えば、ドアや金庫の開閉装置に接続したり、有資格者のみに操作が許された機械・装置などに接続することによって、本認識システムの応用分野を拡大することができる。

【００１９】小型端末１の種類としては、通常、個人が持ち歩くことが可能である電子端末であれば、特に限定されるものではなく、例えば、第１図に示したような小型コンピュータ、携帯ゲーム機、携帯情報端末、携帯電話端末などを例示することができる。

【００２０】赤外線受発光装置１１と同２１の通信可能エリアを、第２図（平面図）に示すように設定すると（赤外線受発光装置１１の通信可能エリアを斜線領域Ａで示し、同２１の通信可能エリアを斜線領域Ｂで示す）、例えば、ｉ)識別対象者３０が、コンピュータ１０の操作を行わず、コンピュータ設置台４０から離れている場合には、通信可能エリアＡ・Ｂは互いに重なり合わず、赤外線受発光装置１１と同２１は通信不能であるので、コンピュータ１０は、識別対象者の不在を検知し、キーボードのロックや画面表示内容の消去、終了処理等セキュリティー確保のために必要な処理が自動的になされている。また、ｉｉ）識別対象者３０が、コンピュータ１０の操作を行う場合には、赤外線受発光装置１１と同２１は、互いの通信可能領域Ａ・Ｂが重なり合うように対峙するので、赤外線受発光装置１１と同２１を介して、コンピュータ１０と小型コンピュータ２０が通信可能となり、識別対象者３０が小型コンピュータ２０において保持している個人識別のための情報が、赤外線受発光装置１１において受信される。そして、この個人識別情報をもとに、コンピュータ１０は自動的に個人識別処理を実行し、識別対象者３０を認識した後は、自動的に１０を操作可能状態とすることができる。本認識システ

ム１００では、上記の例示状態i)とii）を、識別対象者３０の挙動により自動的に切替えることができる。

【００２１】このように、本識別システム１００においては、識別対象者３０が自身の正しい個人識別情報を入力した小型コンピュータ２０を携帯するだけで、識別対象者３０本人が特別な操作や意識をすることさえなく、自動的に適切な個人識別により、所望するシステムのセキュリティー確保が可能である。

【００２２】赤外線通信では、赤外線のビームの強度やビームの幅を調整することで簡単に通信可能範囲をコントロールすることが可能であり、さらに簡単に遮蔽が可能である。

【００２３】第３図は、上記の個人識別端末２が密集している場合の本認識システムの概略図（平面図）である。第３図では、コンピュータ設置台４０'上に、各々上記の赤外線受発光装置ｂが接続されている３台の上記の個人識別端末２が示されている〔コンピュータ１０Ａ（赤外線受発光装置１１Ａが接続されている），同１０Ｂ（赤外線受発光装置１１Ｂが接続されている），同１０Ｃ（赤外線受発光装置１１Ｃが接続されている）〕。また、各々の赤外線受発光装置ｂの近傍に、各々の赤外線受発光装置ｂから発信される赤外線のコンピュータに向かって左側への散乱を遮蔽するべく、赤外線を遮蔽することが可能な小パーティション（６１Ａ，６１Ｂ，６１Ｃ）が設置されている。さらに、各々の赤外線受発光装置ｂから発信される赤外線のコンピュータに向かって右側への散乱を遮蔽するべく、赤外線を遮蔽することが可能な大パーティション（６２Ａ，６２Ｂ，６２Ｃ）が、コンピュータ設置台４０'の手前方向に設置されている。

【００２４】パーティションを、第３図に示すように設置して、赤外線による通信可能領域を、例えば、通信可能領域Ｃ，Ｄ，Ｅのように適宜調整することが可能である。すなわち、この図に示すように、コンピュータ１０が密集して配置されているような場合であっても、パーティション等の赤外線に対する障壁を設けることにより、赤外線による通信可能領域を整理して、相互に混信することなく、複数の認識対象者を容易に、各々の個人識別端末において識別することが可能である。

【００２５】また、一般に赤外線による通信可能領域は、せいぜい数メートル程度であるので、通信可能領域が比較にならないほど広域の電磁波やネットワーク通信を用いる場合よりも、本認識システムの安全度が優れていることは明らかである。

【００２６】そこで、本認識システムの使用の態様として、単純な形式のもの、例えば、（１）適当な時間間隔で間欠的に、個人ＩＤ番号とパスワードを、平文のメッセージとして、赤外線通信により、小型端末１から個人識別端末２に向けて送信し、個人識別端末２が受信内容を確認する。そして、この受信内容が、同端末２に登録

されている個人ＩＤ番号とパスワードと一致すれば、識別対象者であると識別して、次の個人ＩＤ番号とパスワードの受信まで、個人識別端末２が本人識別肯定時の反応する過程を繰り返す、本認識システムの使用を行うことも可能である。

【００２７】すなわち、本発明は、個人識別情報を赤外線通信機構ａから発信させ、この個人識別情報を赤外線通信機構ｂが受信し、かつ、かかる個人識別情報が個人識別端末２における照合により適合とされた場合にのみ、個人識別端末２が本人識別肯定時の反応をすることにより個人の識別を行う、本識別システムの使用方法を提供する発明である。

【００２８】しかしながら、この本システム使用方法は、通信内容を傍受する等の悪意がある第三者が介在する場合等においては、完璧に安全とはいいがたい。例えば、第４図（平面図：記号等は、特に断わらない限り、第２図に準ずる）に示すように、上記のような悪意ある第三者７０が、赤外線受発光装置１１の近傍に、密かに赤外線受光装置７１を設置して、正当な識別対象者３０による赤外線通信の内容を、読み取り装置７２によって、傍受・記録した場合を想定する（図中、８０は、第三者７０による傍受・記録行動を、識別対象者３０などから隠蔽することを可能とする手段、例えば、障壁などを表すものとする）。この場合、識別対象者３０が離席した後に、第三者７０の所有する赤外線通信装置によって、先立って傍受・記録した識別対象者３０のＩＤ番号とパスワードを、赤外線受発光装置１１に向けて発信すれば、第三者７０は、識別対象者３０になりすまし、コンピュータ１０を不正に操作することが可能となることとなる。

【００２９】したがって、機密性や重要度の高い情報を扱うシステムにおいては、このような傍受・盗聴による成りすましができないような工夫が必要になる。このような例としては、例えば、（２）上記の個人識別端末２は、適当な時間間隔で、間欠的に、同じ値が繰り返し出現しないデータ（本発明においては、このようなデータをランダムデータともいう）、例えば、偶発的に同じ値が繰り返すことを防止するのに十分な桁数の疑似乱数やワンタイムパスワードや後述する一方向ハッシュ関数の出力値等を含む情報を、上記の小型端末１に向けて送信し、これを受信した小型端末１は、この情報を、例えば、識別対象者が保有する秘密鍵で暗号化して、この暗号化情報を識別対象者のＩＤ番号と共に、個人識別端末２に向けて送信する。そして、個人識別端末２は、この送信情報を、前記ＩＤ番号から対応する公開鍵を見出して、送信情報を復号して、この復号情報と個人識別端末２が記憶している最初の発信情報とを比較して、両者が一致していれば、識別対象者が真正であることを識別することが可能である。

【００３０】この処理を、間欠的に繰り返し行うと、個

人識別端末２から、小型端末１に向けて、一定間隔毎に、次々に前回とは異なる内容の情報が送信され、小型端末１においては、これらの毎回異なる情報を、自己の秘密鍵で次々と暗号化して、個人識別端末２に向けて送信することとなる。従って、この通信内容の傍受・記録を試みる悪意の第三者が傍受したとしても、かかる第三者は小型端末１における秘密鍵については把握していないので、個人識別端末から次々に送信される情報を正しく暗号化することができず、真正な識別対象者になりすますことは不可能である。

【００３１】すなわち、本発明は、個人識別情報に、ワンタイムパスワード、擬似乱数発生プログラムにより得られる擬似乱数、後述する一方向ハッシュ関数等のランダムデータが含まれ、このランダムデータの照合を個人の識別行為に含めて個人を識別する本識別システムの使用方法、並びに、個人識別情報に暗号化されている情報が含まれ、この暗号化されている情報を照合して個人を識別する本識別システムの使用方法を提供する発明でもある。

【００３２】なお、例えば、暗号化されているランダムデータを用いる本システム使用方法においても、上記のような悪意ある第三者が、長時間にわたり情報の傍受を続け、送信情報の組を全部記録することができれば、原理的には、真正な識別対象者になりすますことが可能とも思われる。しかしながら、ランダムデータのランダム性を十分に大きくすることにより、例えば、ランダムデータとして用いる擬似乱数の桁数を十分大きく設定する（例えば、１０桁程度以上）ことにより、情報を傍受して記録するだけでも膨大な時間がかかるようにすることが可能であり、しかも、適宜秘密鍵の変更等を行うことで、第三者の悪意あるなりすましに対しほぼ完璧に対抗することが可能である。

【００３３】この（２）の方法は双方向の通信と暗号技術を利用して安全性を高めているが、ランダムデータとして、特に、ワンタイムパスワードを利用することで、片方向通信でも同程度の安全性を確保することが可能である。これを例（３）とすると、（３）識別対象者の秘密のパスワードを、個人識別端末２と小型端末１が、共に保有しており、かつ、これらの両端末１・２が共に適性な時計機構を保持しているものとする。そして、小型端末１では、適切な間隔を空けて、間欠的に、その時点での時刻情報と識別対象者の秘密のパスワードを結合し、かかる結合情報を一方向ハッシュ関数に入力してハッシュ値を計算し、その計算結果すなわちワンタイムパスワードにＩＤ情報等を付加した情報を、赤外線受発光装置ｂ・ａを経由させて、個人識別端末２へ送信する。そして、この情報を受信した個人識別端末２は、保有するＩＤ情報を基に対応する識別対象者の秘密のパスワードを検索し、その時点での時刻情報と検索して判明したパスワードを結合し、上記の一方向ハッシュ関数と同一

の関数に入力して、ハッシュ値を算出し、再び得られたハッシュ値と、小型端末１から既に送信されたハッシュ値を比較し、これらのハッシュ値が一致していれば、真正の識別対象者であることを確認することが可能である。

【００３４】この例（３）では、時刻情報を２回用いており、両者の時刻情報が一致している必要があるが、個人識別端末２と小型端末１が保有する時計機構同士の誤差や通信時間のわずかなタイムラグ等が認められるため、時刻情報の単位の設定と許容誤差を適切に定める必要がある。例えば、時刻情報の単位を秒までとし、許容誤差をプラスマイナス１秒以内とした場合は、個人識別端末２において得られたハッシュ値が小型端末１で得られたハッシュ値と不一致であるときに、「個人識別端末２で付加される時刻±１秒」の値を用いて再計算し、それでもハッシュ値が不一致の場合にのみ、識別対象者が非真正者であると結論付けることとなる。

【００３５】なお、一方向ハッシュ関数には、ＣＲＣ、ＭＤ４、ＭＤ５、Ｓｎｅｆｕ、ＳＨＡ－１、チェックサム関数等、いくつかの種類が認められるが、いずれの関数を用いても、計算は非対称鍵暗号等と比べて簡単で処理時間も少なくて済み、ハッシュ値からもとの入力データは算出できず、同じハッシュ値を持つ異なる入力データを見つけることが極めて困難であるという特徴が認められる。

【００３６】このように、本発明は、個人識別情報にワンタイムパスワードが含まれている、上記（１）において述べた個人識別システムの使用方法を提供する発明である。

【００３７】このワンタイムパスワードを使う方法（３）は、（２）の方法に比べ計算量や通信量が少なくて済み効率的であるが、個人識別端末２と小型端末１における時刻情報が一定の誤差以内でなければならず、定期的に時刻合わせをしなければならないという問題も認められる。こうした問題をもたない効率的な方法として次の（４）のような方法も考えられる。

【００３８】（４）個人識別端末２と小型端末１に、全く同一の擬似乱数発生プログラム等のランダムデータの発生プログラムを保有させ、両端末における最初の情報の交換は、非対称鍵暗号等で行い、正しい小型端末１であることの確認と同時に、個人識別端末２から小型端末１へ送る暗号化された情報の中に、ランダムデータの発生プログラムにあたえる初期値（シード値）も含ませる。以後、適切な時間間隔で、小型端末１は、このシード値を基にして、ランダムデータＲ（Ｒ１，Ｒ２，Ｒ３，．．．）を次々に発生させて、ＩＤ情報とランダムデータを含む情報を、暗号化しない状態（平分）で、個人識別端末２に送信する。次に、個人識別端末２でも、同じシード値を同じランダムデータ発生プログラムに与えてランダムデータｒ（ｒ１，ｒ２，ｒ３，．．．）を

計算する。前述したように、両端末ｂ・ａのランダムデータの発生プログラムとシード値が同じであるから、小型端末１から逆転送される正しいＲは、必ずｒと一致することとなる。すなわち、このＲとｒの同一性が維持されている場合には、識別対象者が真正であることを確認することができる。

【００３９】すなわち、本発明は、小型端末１と個人識別端末２が、同一のランダムデータの発生プログラムを保有し、個人識別端末２と小型端末１との間の初期の応答要求メッセージおよび／または応答メッセージに含まれる暗号化されている情報に、前記のランダムデータのシード値となる値を含ませ、以後、小型端末１から個人識別端末２に向けて送られるメッセージに、このシード値を初期値として発生させたランダムデータを含ませ、個人識別端末２においても前記のランダムデータの発生プログラムにより前記のシード値を初期値としたランダムデータを算出し、小型端末１から個人識別端末２に向けて送られる前記のメッセージに含まれるランダムデータと比較照合して、両者のランダムデータが一致した場合に、個人識別端末２が本人識別肯定時の反応をする、本識別システムの使用方法を提供する発明である。

【００４０】この場合、情報の傍受・記録の悪意ある第三者が、両端末ｂ・ａの通信を傍受していたとしても、シード値自体は暗号化されているので、その本当の内容をこの第三者は知ることができず、上記のランダムデータＲを算出することはできない。つまり、上記の悪意の第三者は、真正の認識対象者になりすますことはできないこととなる。

【００４１】この方法（４）では、一度通信が中断した場合等は、暗号化したシード値の交換から再開することになる。なお、もちろん交換するシード値は、個人識別端末２が毎回独自にランダムデータの発生プログラム等により発生させたもので、外部のものが全く予測できない値としなければならない。

【００４２】この方法（４）では、識別プロセスの初期段階のみ双方向通信が必要で、かつ暗号化や復号化といった、比較的演算プロセスが複雑で、電子端末に負担がかかる過程を経なければならないが、以後は通信が中断する等しない限りは、片方向通信で、しかも単純な疑似乱数等のランダムデータを算出するための計算だけで、所望する安全性を確保することができる。

【００４３】前述したとおり、赤外線通信は電磁波等を使う場合に比べて通信エリアを管理し易い特徴がある。しかしながら、それでも、ある個人認識端末２に対し、すでに一人の識別対象者が通信可能領域にあって、この認識対象者が保持する小型端末１による、個人識別の最中に、他の識別対象者が、この通信可能領域に入る可能性も否定できない。よって、このような場合であっても、識別過程が正しく行われるようにする手段を講ずることは、好ましいことである。

【００４４】このような手段として、例えば、以下に述べる方法（５）を例示することができる。（５）個人識別端末２の通信可能領域に誰も識別対象者がいない場合、すなわち、個人識別端末２が個人識別の対象待ちのときには、この個人識別端末は、不特定者に対する応答要求メッセージＧ１を、好ましくは、適切な時間間隔で間欠的に送信する。これを受信した識別対象者が保有する小型端末１は、他の個人識別端末２と通信中であれば、この応答要求メッセージＧ１を無視し、通信中でなければ、このＧ１に対する応答メッセージＦ１を、応答要求メッセージＧ１を発信している個人識別端末２に送信する。この応答メッセージＦ１には、小型端末１が保有している識別対象者のＩＤ情報が含まれているので、以後、個人識別端末２は、そのＦ１を送信してきた小型端末１に向けてのみの応答要求メッセージＧ２を送信する。この応答要求メッセージＧ２には、識別対象者のＩＤ情報が含まれているので、これを受信した小型端末１は、かかるＧ２に含まれているＩＤ情報をチェックし、このメッセージＧ２が自己に向けられたものであることが明らかになった場合のみ、それに対する応答メッセージＦ２を個人識別端末２に送信することとする。

【００４５】このようにすることで、ある個人識別端末２において、既に誰かが個人識別されている最中に、別の識別対象者（小型端末１を保有している）が近づいたとしても、相互の混信等による本システムの誤作動を防止することが可能である。

【００４６】このように、本発明は、応答要求メッセージを赤外線通信機構ｂから発信させ、この応答要求メッセージを赤外線通信機構ａが受信した場合に、小型端末１から個人識別端末２に向けて応答メッセージを送信させ、この応答メッセージが個人識別端末２において適合とされた場合にのみ、個人識別端末２が本人識別肯定時の反応をすることにより個人の識別を行う、本識別システムの使用方法を提供し、さらには、個人識別端末２が個人を識別している場合のみ、この個人識別端末２に、識別対象の小型端末１に対して特異的な応答要求メッセージを発信させて、これにより小型端末１を、かかる個人識別端末２からの特異的な応答要求メッセージのみに対して応答メッセージを発信するようにし、さらに個人識別端末２を、この小型端末１からの応答メッセージのみに呼応可能な状態とし、かつ、個人識別端末２が個人を識別していない場合には、個人識別端末２に、不特定の小型端末１に対する応答要求メッセージを発信させ、小型端末１を、この対象不特定の応答要求メッセージのみに呼応可能な状態とする、上記の本識別システムの使用方法を提供する発明である。

【００４７】また、①上記の応答要求メッセージおよび／または応答メッセージに、ランダムデータ（ワンタイムパスワード、擬似乱数発生プログラムにより得られる擬似乱数、一方向ハッシュ関数の出力値等）が含まれ、

このランダムデータの照合を個人の識別行為に含めることが好ましく、また、②応答要求メッセージおよび／または応答メッセージに暗号化されている情報が含まれ、この暗号化されている情報を照合して個人を識別することが好ましく、さらには、③応答要求メッセージの発信が間欠的な発信であり、ｉ）これに対する応答メッセージが個人識別端末２において不適合とされた時点で、および／または、ｉｉ）これに対する応答メッセージを、個人識別端末２が受信できなくなった時点で、個人識別端末２が本人識別否定時の反応をすることにより個人の識別を行うことが好ましい。

【００４８】そして、本発明は、この好ましい態様において、個人識別端末２から間欠的に発信される応答要求メッセージの一部に応答要求メッセージ毎に異なる情報が含まれており、かつ、個々の応答要求メッセージに対して小型端末１から発信される応答メッセージに、前記の情報を若しくはこの情報を加工した情報を暗号化した情報が含まれており、この応答メッセージを個人識別端末２が受信した際に、前記の暗号化された情報を複号して、この複号情報と前記の応答要求メッセージに含まれる情報と比較照合して、両情報が実質的に同一である場合に、個人識別端末２が本人識別肯定時の反応を行う、上記の本識別システムの使用方法を提供する発明である。

【００４９】個人識別端末２の通信可能領域に誰もいない状態、すなわち、個人識別端末２が識別待ちの状態のとき、この個人識別端末２は、常に適切な時間間隔で、不特定者に対する応答要求メッセージを、間欠的に送信し続けることになるが、一般的に、個人識別端末２は、すでに図面を用いて述べたように、机上等に設置された電子端末であることが多く、交流電源が供給されている場合が多く、メッセージの連続送信は特に問題とはならない。一方、小型端末１は、携帯型の電子端末であり、バッテリーの容量に限界があるので、パワーを消費する赤外線の送信量は極力押さえることが好ましい。上述した（５）の例では、小型端末１が、個人識別端末２に向けて赤外線を送信するのは、応答要求メッセージＧ１・Ｇ２を受信したときのみである。識別対象者が、いずれの個人識別端末においても、非識別状態の場合、具体的には、例えば、その小型端末１を保有している識別対象者が、食事や会議等をしていて、長時間、個人識別端末２に連動する作業をしない場合等には、小型端末１は、任意の個人識別端末２からの不特定者向けの応答要求メッセージを受信待ちの状態であり、赤外線の送信は行われない。このため、この（５）の手段は、小型端末１のバッテリー持続時間を延長する意味においても有効である。

【００５０】これまで述べてきたような例の他に、小型端末１と個人識別端末２とが個人識別のために交換する情報として、ネットワーク認証プロトコルとして標準になりつつあるＫｅｒｂｅｒｏｓ等を用いることができる。

【００５１】本識別システムは、特定の個人を認識して働く電子情報システムにおける個人識別システムとして非常に有用である。本識別システムの使用対象となる電子情報システムは、全く限定されないが、特に、機密性が高く、なおかつ、電子情報システムの使用者が多忙で、このシステムのＯＮ／ＯＦＦを頻繁に行うことが想定されるシステム、例えば、電子カルテ、銀行システム、証券システム、軍事システム等に用いるのに好適である。

【００５２】

【実施例】以下、本発明を実施例を用いて、さらに具体的に説明する。ただし、この実施例は、本発明の技術的範囲を限定解釈するべきものではない。本発明は個人識別が必要なあらゆる局面で有用であることは、上述した通りであるが、本実施例においては、最も厳しいセキュリティー管理が必要なシステムの一つである、電子カルテ等を扱う医療システムを例にとって説明する。

【００５３】医療システムは、人の生命にかかわる重要な情報を扱うシステムであり、また、患者のプライバシー保護や病名告知問題等、情報のセキュリティーには、特に注意を要するシステムである。しかしながら、このシステムを扱う医師や看護婦は非常に忙しく、例えば、医師が、診療情報を電子カルテシステムに入力中に、急患や入院容体の変化等のために、急いで、しかも数時間も離席することは、日常茶飯事である。従って、このようなシステムにおいて、従来のＩＣカード等による個人識別・認証を行っても、医師がうっかりＩＣカードが挿入されたまま、システム端末から離れてしまうと、システムがＯＮの状態のまま放置されることとなり、誰でも自由にシステムを操作できることとなってしまい、セキュリティー上、大きな問題となっている。

【００５４】本実施例は、このような医療現場における本識別システムの重要性を鑑みた実施態様である。前述した第２図において、本識別システム１００における識別対象者３０（原則として複数：具体的には、医師、看護婦、検査技師等）全員に、赤外線通信機能を有する小型の携帯型コンピュータ２０を配布する。システムの管理者（図示せず）は、識別対象者３０全員に、非対称鍵暗号の鍵のペア（公開鍵P-key と秘密鍵S-key ）を一組づつ割り当て、携帯型コンピュータ２０には、識別対象者３０の配布前に、これらの対象者のＩＤ（職員番号等）とS-key を登録しておく。

【００５５】また、システム管理者以外は、携帯型コンピュータ２０のS-key の内容を見たり、変更できないようにしてある。さらに、医療システムのコンピュータ１０には、識別対象者３０全員のＩＤとP-key の対応表を登録しておき、特定のＩＤをもつ職員のP-key を、コンピュータ１０において参照できるようにする。

【００５６】コンピュータ１０は、本識別システム１００を用いる病院内の要所要所（例えば、診察室、手術室、検査室、ナースステーション、事務室等）に、好適には複数台設置されている（各々のコンピュータ１０は、電子的に情報交換をすることが可能な機能を備えていることが好ましい）。なお、各々のコンピュータ１０には、個別のＩＤ（端末番号等）が入力されている。また、全てのコンピュータ１０には、赤外線受発光装置１１が、直接的若しくは間接的に接続されている。

【００５７】識別待ちの状態では、コンピュータ１０は、不特定者に対する応答要求メッセージＧ１：

Ｇ１：Ａ００１１

（コンピュータ１０のＩＤが「Ａ００１１」の場合）を、短い時間間隔、例えば、０．１秒間隔程度で赤外線によって送信し続ける（時間間隔を短くすることで、認証対象者３０がコンピュータ１０に近づいたときの反応を早くすることができる）。

【００５８】例えば、診察室に一台のコンピュータ１０が設置されている。識別対象者である医師３０が、自分のＩＤ情報とS-key が登録された正しい携帯型コンピュータ２０を胸につけている。携帯型コンピュータ２０にも赤外線受発光装置２１が接続されているが、何処かのコンピュータ１０から、応答要求メッセージＧ１を受信するまでは、何も送信しない受信待ち状態となっている。

【００５９】医師３０が診察室に入り、コンピュータ１０に近づいて、赤外線受発光装置１１と２１が通信可能な位置関係〔第２図（２）〕になると、携帯型コンピュータ２０は、赤外線受発光装置１１・２１を介して、コンピュータ１０から応答要求メッセージＧ１を受信し、ただちに応答メッセージＦ１：

Ｆ１：Ｄ０１３５：Ａ００１１

（医師３０のＩＤが「Ｄ０１３５」の場合）を赤外線受発光装置２１・１１を介してコンピュータ１０へ向けて送信する。応答メッセージＦ１には、医師３０のＩＤ情報が含まれているので、コンピュータ１０では、登録されている各認識対象者のＩＤを検索して、医師３０のＩＤに対応するP-key を見出し、このP-key によって暗号化したメッセージＲを含むメッセージＧ２：

Ｇ２：Ｄ０１３５：Ａ００１１：3eb%78xdc-92ef

（Ｓ＝7359224781で、これを暗号化したＲが「3eb%78xdc-92ef」の場合）を携帯型コンピュータ２０へ送信する。この実施例では、コンピュータ１０が応答メッセージＦ１を受信したときに発生させた擬似乱数文字列Ｓを暗号化したものをＲとしている。

【００６０】このメッセージＧ２を受信した携帯型コンピュータ２０は、これに登録されているS-key によって、メッセージＧ２に含まれているメッセージＲを復号し、文字列Ｓを得る。メッセージＲを正しく復号できるのは、秘密鍵S-key を持つ携帯型コンピュータ２０だけであるから、この段階で、１０と２０は他者に知られていない秘密の情報Ｓを正しく共有することとなる。携帯型コンピュータ２０は、メッセージＧ２を正しく受信し、準備が完了したことをコンピュータ１０に知らせるため応答メッセージＦ２：

Ｆ２：Ｄ０１３５：Ａ００１１

をコンピュータ１０へ向けて送信する。

【００６１】応答メッセージＦ２を受信したコンピュータ１０は、以後、間欠的に応答要求メッセージＧ３：

Ｇ３：Ｄ０１３５：Ａ００１１：１６３

（ＳＥＱが「１６３」の場合）を、携帯型コンピュータ３０へ送信する。応答要求メッセージＧ３には、ＳＥＱというフィールドが含まれているが、これは、コンピュータ１０が送信する何回目かのＧ３であるかを示すシーケンスナンバーであり、一種のカウンターである。

【００６２】応答要求メッセージＧ３を受信した、携帯型コンピュータ２０は、前述した共有秘密の文字列Ｓを基に、一方向ハッシュ関数であるＭＤ５を用いて、コンピュータ１０と携帯型コンピュータ２０しか算出できない値Ｈを算出して、このＨを含む応答メッセージＦ３：

Ｆ３：Ｄ０１３５：Ａ００１１：１６３:9e3bcf73d48f99eca865465caf679e77

をコンピュータ１０へ送信する。このとき、仮に、前記メッセージＧ３やＦ３を第三者に傍受されたとしても、次に送るべきＦ３が第三者には予測できないようにすることが、セキュリティー上好適である。かかる予測不能化手段として、前述したランダムデータ（これを暗号化してよい）があるが、非ランダムデータであっても、これを一方向ハッシュ関数（前述した）で処理した出力値で予測不能化することもできる。一方向ハッシュ関数は、入力データが全く同じであれば同じハッシュ値を出力値として算出するが、例えば、上記例のように、ＭＤ５の出力するハッシュ値は１２８ビット（１６進数表示で３２桁）という大きな数値であり、入力データが少しでも違うと全く異なったハッシュ値を出力する。またハッシュ値から入力データを導出したり予測することはできない。

【００６３】応答メッセージＦ３において、ＳＥＱは、直前に受信した応答要求メッセージＧ３に含まれているＳＥＱと同じ値である。コンピュータ１０と携帯型コンピュータ２０の間で、文字列Ｓの内容を交換した後、最初の応答要求メッセージＧ３のＳＥＱが１で、以降、２、３、４、．．．と順次１づつ値が増えていく。次に、値Ｈは、文字列ＳとＳＥＱを結合して得られる情報を、一方向ハッシュ関数ＭＤ５に入力して算出されるハッシュ値である。この場合、文字列Ｓ＝７３５９２２４７８１であるとすると、最初に送信する応答メッセージＦ３のＨは、ＭＤ５（7359224781-1）で計算され、「fc4d94633e5f4128959e3d6a77fde4eb」が算出される。

【００６４】同様に、２番目に送信する応答メッセージ

Ｆ３のＨは、ＭＤ５（7359224781-2）で計算され、「5baab4f5876b1ee9869e0b02ceccbe8e」が算出される。

【００６５】この例でも判るように、入力データは末尾であるＳＥＱの１が２に変わっただけであるが、ハッシュ値は全く異なった値となっており、しかも、次に、ＳＥＱが３に変わったときのＨは、正しいＳを知らなければ計算できない。

【００６６】この例では、応答メッセージＦ３は、ハッシュ値Ｈと、先に述べたＳＥＱ、さらにメッセージの識別用に、医師３０のＩＤ番号と、コンピュータ１０のＩＤ番号からなっている。

【００６７】応答メッセージＦ３を受信したコンピュータ１０は、まず識別用のＩＤ番号をチェックして、それが自分宛てのメッセージであり、かつ、いま識別しようとしている医師２０からのものであることを確認する。さらに、応答メッセージＦ３に含まれるＳＥＱが、直前に自身が送った応答要求メッセージＧ３のＳＥＱと一致していることを、コンピュータ１０は確認する。かかる一致が認められた後、そのＳＥＱとコンピュータ１０自身が保持している秘密の値Ｓを、携帯コンピュータ２０と同様にして、一方向ハッシュ関数ＭＤ５に入力して、ハッシュ値ｈを算出する。算出されたｈと、応答メッセージＦ３に含まれているＨとを比較照合し、もし両者のハッシュ値が一致していれば、医師３０が個人として識別されたものとして、コンピュータ１０は、識別肯定時の処理、すなわちシステムの操作や表示を許すようにする。

【００６８】なお、本実施例において、システムのセキュリティーを維持するため、コンピュータ１０は、可能な限り短い時間間隔で、次々に応答要求メッセージＧ３を送信し、これらに対して各々返送されてくる応答メッセージＦ３を確認すべきである。しかしながら、コンピュータ１０および携帯型コンピュータ３０が、計算や通信のためにＣＰＵの計算パワーやバッテリーを消費するので、要求されるセキュリティーレベルやシステムの運用に応じた適切な時間間隔、本実施例においては、０．５～２秒程度に設定するのが好ましい。

【００６９】仮に、ハッシュ値ｈとＨが不一致の場合は、何らかの不正が働いている可能性が認められるので、コンピュータ１０は、ただちに個人識別否定時の処理、すなわち表示内容の消去やシステム操作を不能とする処理等を行うこととなる。また、応答要求メッセージＧ３送信後、所定の時間（例えば、０．１～０．５秒程度）が経過しても、コンピュータ１０が応答メッセージＦ３を受信できない場合にも、ただちに、上記の個人識別否定時の処理を実行することもできる。ただし、医師３０のささいな動作等によっても、瞬間的に通信が中断する場合等も考えられるので、応答要求メッセージＧ３を再送して、応答メッセージＦ３を再度待つという、リトライ処理を行うこともできる。かかるリトライの回数

や時間間隔等は運用に適した値を設定することができるが、概ね、リトライ回数が２～１０回程度、時間間隔が０．２～５秒程度が好ましい。

【００７０】また、個人識別が否定された場合、個人識別プロセスは、初期状態に戻ることとなる。すなわち、コンピュータ１０は、かかる否定前に識別していた医師３０のＩＤ情報やＳおよびＳＥＱ等を全て破棄し、再び、不特定者に対する応答要求メッセージＧ１を送信することになる。一方、携帯コンピュータ２０も、それまで識別していたコンピュータ１０からの応答要求メッセージＧ３が、所定の時間（概ね３～３０秒程度）受信できなければ、それまで保持していたＳや、コンピュータ１０のＩＤ情報等を破棄し、応答要求メッセージＧ１の受信待ち状態（初期状態）に戻ることとなる。

【００７１】ただし、このように個人識別が否定された場合、コンピュータ１０の業務プログラムを強制終了するようにすることも可能であるが、例えば、このような場合であっても、個人識別否定中にコンピュータディスプレーの画面表示や操作ができないようにしておくことで、実質的に目的を達成することもできる。例えば、個人識別否定から一定時間内であれば、同一人物が個人識別プロセスを初期状態から行って、再度、個人識別が肯定されたときに、個人識別が否定される直前の状態から業務プログラムを再開できるようにしてもよい。これは、例えば、医師３０が、患者の診療録情報を入力中に、簡単な検査が必要になって２～３分離席し、引き続いてその患者の診療録情報入力を再開したいような場合が想定される。

【００７２】このように、本実施例では、通信の主導権は、コンピュータ１０にあり、通常、携帯型コンピュータ２０側は待機状態であり、コンピュータ１０から適切な応答要求メッセージを受信したときにのみ、これに対する応答メッセージを、コンピュータ１０に向けて送信するという態様をとっている。これは、例えば、医師３０が、診察室に設置してあるコンピュータ１０と手術室に設置してあるコンピュータ１０の両方を使うような場合、それぞれの室に要求されるセキュリティーレベルに応じて、応答要求メッセージＧ３の発信時間の間隔やリトライ回数等を適切に調整しておくだけで、医師３０は、１つの携帯型コンピュータ２０を付けたままで、どちらの室へ行っても適切な個人識別を受けることができる。

【００７３】また、上述したように、携帯型コンピュータ２０は、初期状態においては、不特定対象の応答要求メッセージＧ１メッセージのみを受付け、かかる応答要求メッセージＧ１受付け後は、そのＧ１を送信したコンピュータ１０からの応答要求メッセージＧ２のみを受付け、応答要求メッセージＧ２受付後は、そのＧ２を送出したコンピュータ１０からの応答要求メッセージＧ３のみを受け付け、他のメッセージは無視される。

19

【００７４】したがって、あるコンピュータ１０と医師３０の携帯するコンピュータ２０が個人識別状態で、互いに応答要求メッセージＧ３と応答メッセージＦ３を交換し続けているいる状況において、他の者、例えば、看護婦が、その通信可能領域Ａ・Ｂ内に入ってきたとしても、この看護婦が携帯している携帯型コンピュータは、コンピュータ１０から送信されてくる応答要求メッセージＧ３を無視し、全く反応しないので、混信等によって、コンピュータ１０と携帯型コンピュータ３０の間の個人識別が妨げられることはなく、逆に、誤って、この看護婦がコンピュータ１０において個人認証されるということもない。

【００７５】

20

【発明の効果】本発明により、電子システムを操作しようとしている者を、間違いなく本人識別され得る機能が、低コストで、確実に、しかも操作者にとって簡便に実行され得る手段が提供される。

【図面の簡単な説明】

【図１】本認識システムの概要を示す図面（正面図）である。

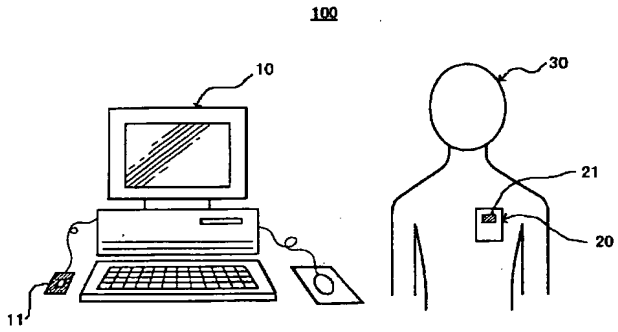
【図２】本認識システムの概要を示す図面（平面図）である。

【図３】個人識別端末が密集している場合の本認識システムの概略図（平面図）である。

【図４】悪意ある第三者の存在を想定した本認識システムの概略図（平面図）である。

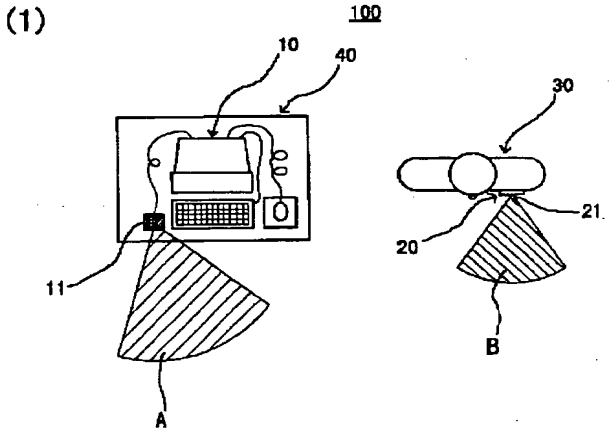
【図１】

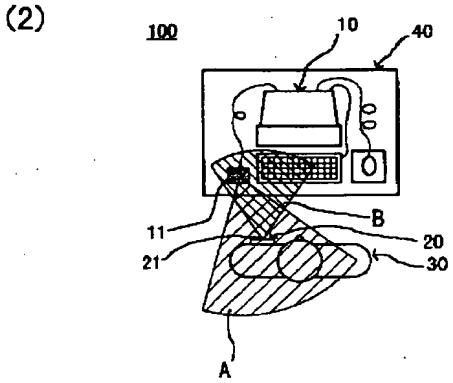
第 １ 図



【図２】

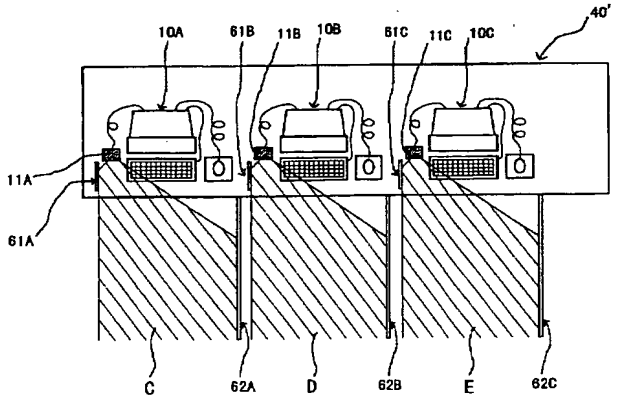
第 ２ 図





【図３】

第 ３ 図



【図４】

第 4 図